Havells India

Third Party Security Policy

Version 1.0

Document Statistics

S. No.	Type of Information	Document Data
1.	Document Title	Havells India Third Party Security Policy
2.	Document Code	HTPSP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No.	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Document Scope

This document shall be applicable to the IT department and the employees/third parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose

The purpose of Third Party Security Policy is to provide and establish information security compliance guidelines for IT department of Havells and the associated third party service providers who handle or have access to Havells' data/information systems, and/or information assets.

1.1 Scope

This policy shall be applicable to the IT department and the employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in this policy.

1.3 Enforcement

All employees and/or third party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.

b) Employees and Third Parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy.*

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

1.5 Definitions

a) Third Party employees: Third party refers to any entity (supplier, vendors, contractual employees, etc.) with whom Havells engages in a business relationship to deliver product and services to its customers;

b) Supplier: Supplier refers to a firm/company/organization with whom Havells contracts to purchase goods and/or services; and

c) Contractor: Contractor refers to a person/ independent contractor/consultant or a firm/company/organization that works on a contractual basis with Havells to work on specific jobs or projects for a fixed time frame and have a defined scope of work.

2. Policy

The objective of Third Party Security Policy is to protect Havells' data and/or information assets that are accessible to or affected by the third party employees.

Havells must identify and manage information risk throughout each stage of relationship with third party. Havells shall accomplish this primarily by embedding information security requirements in formal contracts or legal agreements and obtaining assurance that they are met.

2.1 Onboarding third parties

a) Havells shall draw and sign formal written contracts / digital contracts / confirmation via email with all the third-party service providers. These contracts shall include the Service Level Agreement (SLA) identified, defined and agreed on for the respective service wherever applicable;
b) The third party shall ensure that their employees/agents complete information security formal or informal training (provided by third party or Havells) prior to deployment on Havells' engagement; and
c) Third party employees shall be provided access to Havells' systems or allocated any Havells' assets as per business requirements or on request from business team post business justification.

2.1.1 General requirement for all third parties

The following section is applicable to all third parties:

2.1.1.1 Non-disclosure agreements

All third-parties must contractually agree to maintain strict confidentiality (e.g. through a Non-Disclosure Agreement (NDA)) /MSA (Master Service agreement concerning Havells' information.

Refer: Code of Conduct including NDA, Code of Ethics

2.1.1.2 Delegation of responsibility

Third-parties shall be responsible to ensure that Havells' reputation, interests, information and IT assets are protected against loss, theft, disclosure and unauthorized access as per the defined guidelines provided by Havells. This includes any other parties that they may employ as sub-contractors or agents.

2.1.1.3 Access and asset management

The below listed guidelines shall be followed for providing assets or logical access to third party employees after signing the contract:

a) By default, all laptops allocated to third party staff will have USB ports blocked;
b) The internet access for all third-party staff will be restricted as per the acceptable usage policy;
c) Remote/VPN access shall be granted post management's approval;

Refer: Access control policy

2.1.1.4 Relationship Manager

Third party shall appoint a relationship manager who will act as the single point of communication with Havells' IT team wherever applicable.

2.1.1.5 Data Security

a) Third Party who access information generated, stored and processed within Havells, shall be made aware of information security responsibilities through communication of relevant information security guild lines / polices ;
b) Havells' confidential data must only be handled and stored at the contractually agreed sites and backup storage sites.

2.2 During employment of third parties

a) Third party employees/agents shall ensure, at all times, that Havells' data is handled as per the defined guidelines provided by the process owners;
b) Periodic management review meetings shall be conducted between third party and Havells' IT team to track compliance to SLAs as agreed with Havells;
c) Third parties shall maintain confidentiality, integrity and availability of Havells' information and assets.

Refer: Acceptable usage policy, Asset Management policy, Network Security Management Policy

2.3 Off-boarding third parties

a) There should be an exit plan and the terms on which Havells has a right to terminate the contract or legal agreement;
b) Third party shall serve a minimum notice period (agreed upon with Havells) before terminating the contract;
c) At the time of off-boarding, the third party must provide relevant documents and conduct knowledge transfer sessions to smoothly transition out;
d) All assets provided to third parties, must be returned at the time of off-boarding;
e) Havells shall ensure that all the access rights defined/provided to third party resources shall be revoked upon separation of third-party resource and/or termination of third-party services.

2.4 Managing Changes to Third Party Services

Changes to the contracts with Strategic partners/third parties shall be reviewed and approved in accordance with this policy and as per delegation of authority *(refer DOA)*.